Initiative for State Infrastructure Protection (ISIP)
Vulnerability Alert Process (VAP)
Concept of Operations

In Support of the ISIP Concept of Operations

Director, Information Assurance Division
Office of the Chief Information Officer/G6
Headquarter s, Department of the Army

Purpose: To establish basic steps, procedures, and dissemination processes for the sharing of Department of Defense (DoD) Information Assurance Vulnerability Alerts (IAVA), Information Assurance Vulnerability Bulletins (IAVB), and Technical Advisories (TA) to any state cyber infrastructure protection agency as a proactive deterrent for cyber threats and attacks on commercial information systems and networks in accordance with the tenets of the Initiative for State Infrastructure Protection (ISIP) program.

General: Maintaining awareness of new threats and vulnerabilities requires daily examination and analysis of reputable information sources. Validating the threat, assessing its potential impact, and determining remediation steps, patches and upgrades that must be tracked and managed for every device, operating system and application is exhaustive in terms of manpower and budget. All too often, this immense task falls entirely upon those who are maintaining the enterprise networks.

Within its scope of operations, the DoD funded Initiative for State Infrastructure Protection program, through its affiliation with the National Guard Emergency Operations Centers (EOC) or Computer Emergency Response Teams (CERT), offers a centralized vulnerability notification and management capability—the ISIP VAP. The ISIP VAP helps to reduce the burden on State security staff and allows them to focus on other critical tasks.

Vulnerability Alert Notification Process

There are three types of Vulnerability Alert notifications generated by the DoD Computer Emergency Response Team (CERT) (*see Appendix A*):

Information Assurance Vulnerability Alert (IAVA): An IAVA message is generated when network vulnerability is severe, resulting in an immediate potentially severe threat to systems and information. Due to the severity of the risk presented by these vulnerabilities, corrective action is of the highest priority.

Information Assurance Vulnerability Bulletin (IAVB): An IAVB addresses new vulnerabilities that do not pose an immediate risk to information systems, but are significant enough that noncompliance with the corrective action could escalate the risk. The local cyber threat manager makes compliance requirements and decisions to disseminate the bulletin enterprise wide.

Technical Advisory (TA): TA is generated when new vulnerabilities exist but are generally categorized as low risk. Potential escalation of these vulnerabilities is deemed unlikely, but the advisories are issued so that any risk of escalation in the future can be mitigated. Specific technical questions regarding individual vulnerability notices should be addressed to the local National Guard CERT.

Benefits of IAVA Subscription

Since its inception in 1998, the automated DoD Vulnerability Alert process (IAVA, IAVB,TA) has enabled DoD information security administrators to assess vulnerabilities, mitigate security risks, lessen critical business impact, and in some cases defend against the attack entirely.

Quick notification and dissemination of vulnerability alert information from the DoD CERT throughout DoD allows the distributed CERT teams to keep abreast of developments that impact on critical systems through advisories, respond faster with system alert notifications, patches, and strengthen ongoing security processes.

Subscribers to the ISIP VAP benefit from:

- Access near to real-time threat and vulnerability alerts that will enable state and local governments to take a proactive approach to network security
- Vendor specific intelligence relevant to the affected environment for a quick response
- Detailed reports of vulnerabilities from the most technically complete database with specific exploit type, date, and method of payload delivery, patch and fix information, credibility, mitigation, resources, and impact rating
- Vulnerability analysis and accurate metrics
- A process that's flexible and can be easily adapted to fit each state's specific needs
- Low Cost or free to state governments.

Subscription / Registration

Each State Cyber Protection manager is required to register directly with the ISIP VAP Website and establish a VAP sharing process via its local National Guard CERT as agreed upon between the two entities.

ISIP Vulnerability Assessment / Implementation Process

The ISIP vulnerability assessment process provides positive control of vulnerability notifications and corresponding corrective actions for DoD and non-governmental network assets. The following describe the organizational flow, generation process, registration, compliance criteria, validation, and verification procedures:

Step-by-Step Implementation Process
(DoD CERT to State National Guard Emergency Operations Center / CERT)

DoD Computer Emergency Response Team assesses a reported or identified vulnerability based on its organizational impact, severity, and means of correcting or mitigating the operational risk associated with it. The DoD CERT will issue one of three messages based on the results of their analysis:

- IAVA – Requires acknowledgement and compliance
- IAVB – Requires acknowledgement only
- TA – Notification only

The DoD CERT then notifies each Combatant Commander, Military Service, and DoD Agency that an IAVA, IAVB, or TA has been issued and are directed to the DoD CERT Web Page for specific details of the message.

Each Combatant Commander, Military Service, and DoD Agency must follow a five step process to ensure that the vulnerability is either corrected or mitigated. That process consists of:

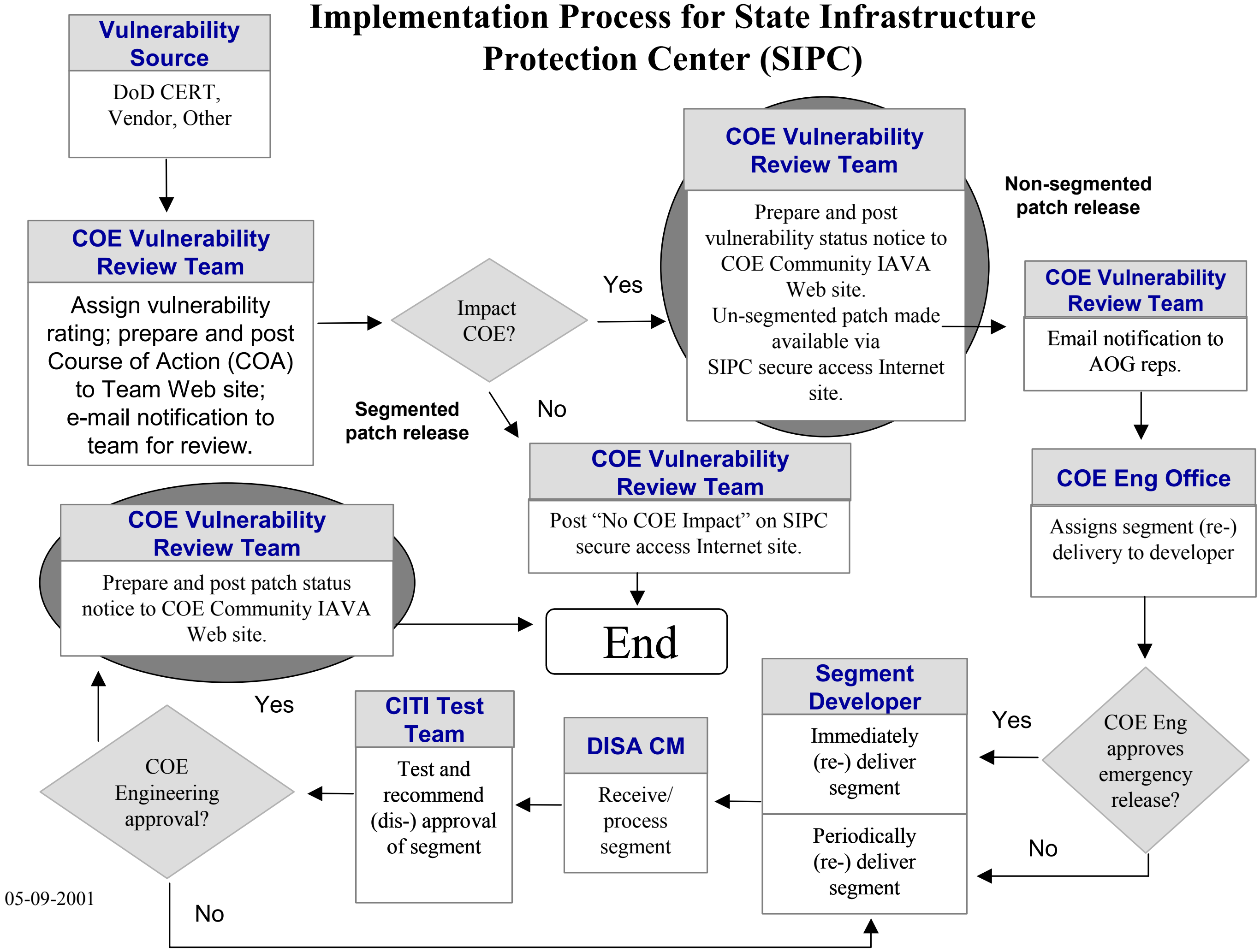
1. Access the DoD CERT Web Page and retrieve the entire vulnerability notice.
2. Notify appropriate security personnel within their organization of the vulnerability notice and inform them to retrieve the message from the DoD CERT Web Page.
3. Acknowledge receipt of the vulnerability notice to the DoD CERT Web Page. Acknowledgment of receipt of the vulnerability notice must be completed within five days unless otherwise specified.
4. Assess the impact of the vulnerability and apply the fix as outlined in the message. If the fix cannot be applied or if more time is needed an extension must be requested if corrective actions cannot be implemented with the specified time allotted.
5. Random compliance checks must be conducted to ensure that random compliance checks on assets to validate the information being reported.

IAVA Review Team assigns vulnerability rating, posts courses of action, assesses impact on environment and assigns review according to the following scenarios:

1. If environment is impacted, pushes to IAVA Review Team for further study.
2. If environment is *not* impacted, IAVA Review Team posts a “no impact” on community website.
3. If Scenario 1 applies:
   i. IAVA Review Team prepares and posts vulnerability status notice and an un-segmented patch to the Engineering Team which assigns segment delivery or redelivery to developer.
   ii. Engineering approves emergency release to Segment Developer to either deliver immediately or periodically.
   iii. Segment Developer determines status of release to DISA Configuration Manager.

iv. DISA Configuration Manager processes segment to Test Team.
v. Test Team tests and recommends approval or disapproval of segment to Engineering.
vi. If approved, Engineering forwards to IAVA Review Team.
vii. If Engineering does *not* approve segment, it reverts to Segment Developer.
viii. IAVA Review Team will prepare and post Patch Status Notices to CERTs organization-wide.
ix. National Guard EOC/CERT will review and purge classified data (if any) from IAVA notifications to disseminate to respective subscriber lists in State Infrastructure Protection Center (SIPC) or SIPC-like private portal.

Common Operating Environment (COE) IAVA Implementation Process for State Infrastructure Protection Center (SIPC)



State National Guard EOC/CERT to State Infrastructure Protection Center
Step-by-Step Implementation Process

A critical component of securing information systems includes the establishment of a central point of coordination. Such an office is a nexus between the federal government and the agencies and private industries within a state. One form that this office may take is a State Infrastructure Protection Center (SIPC).

SIPC could be chaired by a state CIO and consist of a board of directors that include members of state agencies and private industries. This yields coordination of efforts across domains of responsibility, since those agencies directly involved can shape the solutions that will protect them all collectively. In addition, SIPC can work in conjunction with a state Chief Information Office/Chief Technology Office to integrate independent infrastructures into a comprehensive "information grid."

A centralized--such as an SIPC--coordination office has a symmetric benefit: an accurate picture of the "enterprise." Each information system of a state's agencies and private industries are interconnected in unique ways that should be considered as "one state-wide network." "Nodes" are points at which systems connect directly with other systems. A vulnerability in one system is shared by all of the other systems. Each state agency and private industry shares an implicit responsibility to secure their systems. Likewise, it is in the self-interest of each agency and industry to help each other in securing the "enterprise" that they all share.

The core of SIPC includes the National Guard Computer Emergency Response Team (CERT). Each state has its own Army/Air National Guard CERT. The CERTs receive training and network security information from the Department of Defense. The members of a state's National Guard are "dual-hatted." In other words, they are civilians with regular careers and also serve as soldiers. Many of them are information systems security professionals in their regular jobs. Since the National Guard is a state-controlled resource, the National Guard CERT could be mobilized to work with civilian agencies in response to a significant attack. The expertise of the CERTs bridges both private industry and the Department of Defense. A key process is the Information Assurance Vulnerability Alerts (IAVA). These contain network security information that is tailored to mitigate vulnerabilities in specific hardware/software configurations.

The SIPC or other centralized state office can perform certain functions in disseminating network security information across the enterprise of state and private industry networks.

The SIPC is designed with the following functions:

Subscription*:*
Achieve buy-in (subscription) from state agencies and private industries to cooperate with the SIPC

Coordination/Identification:
Assess the topologies ("map the networks") of subscribers for nodes of vulnerabilities

Risk Assessment and Impact:
Conduct a self-assessment of the computing environment/enterprise to determine threat, impact, and applicability of the IAVA alert.

Implementation:
Receive and catalog IAVAs and other information from the National Guard and other trusted sources

Distribution*:*
Disseminate IAVAs to specific subscriber vulnerabilities
Notify subscribers of their relevant IAVAs, with instructions to download/acknowledge IAVAs from a centrally located SIPC "portal"

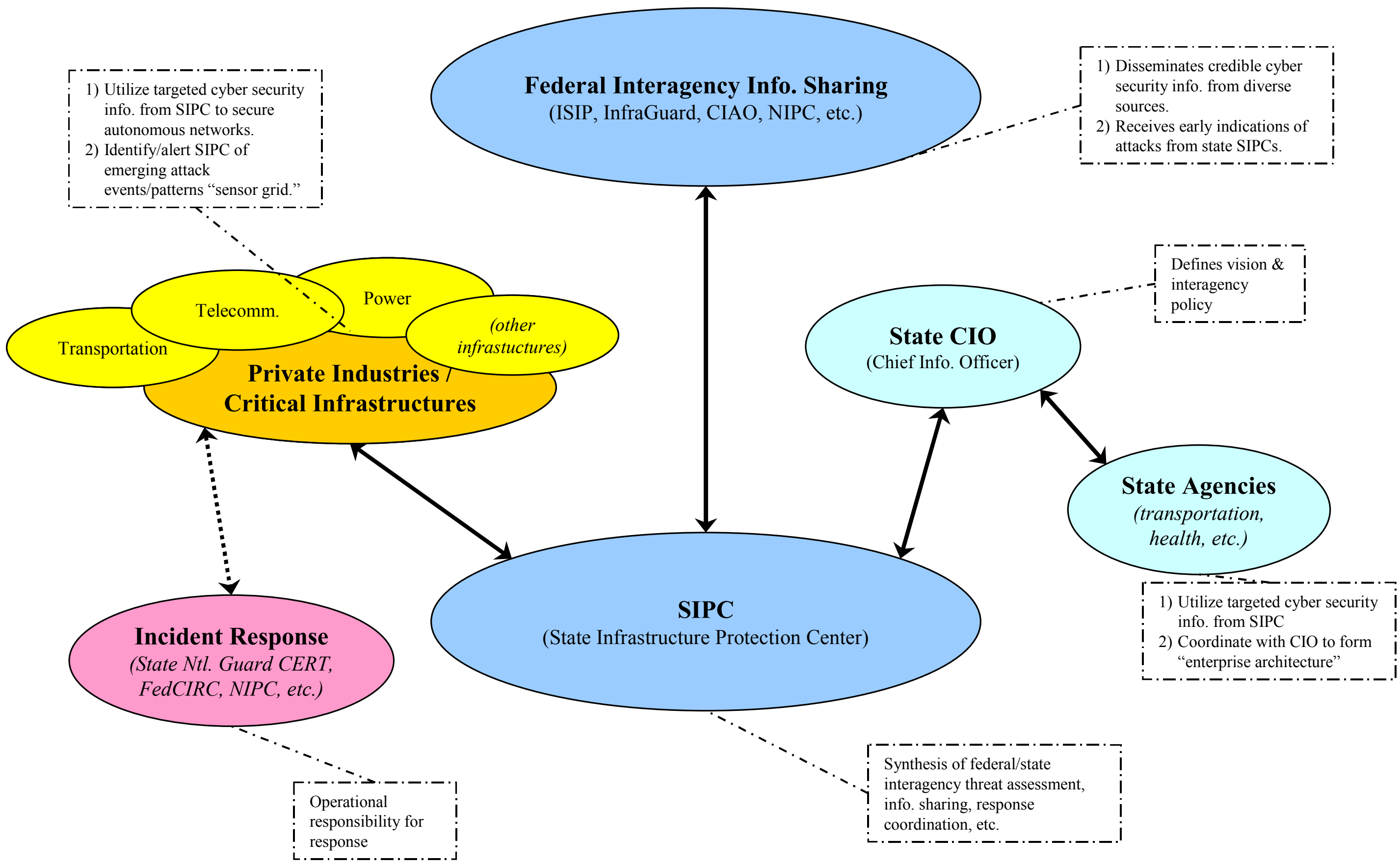
Communication*:*
Receive vulnerability assessments from member agencies to identify and track significant patterns of malicious activity

Return Flow of Information -- Subscribers to the SIPC & National Guard CERT

The subscribers to SIPC represent intrusion detection/prevention systems for the enterprise. This return flow of information is critical to accurately identify vulnerabilities and to identify/analyze threat patterns. It is integral to mitigating attacks. Cooperation of subscribers includes submitting reports and information regarding exploitations of their networks. Information collected from the subscribers will be received and processed by the National Guard CERT team. Since the National Guard is exempt from Freedom of Information Act (FOIA), the information collected remains anonymous. The process of reporting incidents to the SIPC is as follows (see "Two-Way Information Sharing"):

1. Collect "forensics evidence" of the attacks.
2. "Sanitize" the specific identity of the subscriber, while identifying the sector or category of the targeted agency/industry.
3. Submit standardized reports to the SIPC, including general information of the methods and targets of attacks.
4. Inform National Guard CERT of your posting.

Two-Way Information Sharing



<u>Self /Risk Assessment</u>

Agencies are advised to conduct a self-assessment of the computing environment/enterprise to determine relevancy and applicability of the IAVA/ISIP VAP alert.

<u>Legal</u>

There is no legal impediment for sharing information between federal, state, or local governments.

The ISIP was developed by the Defense Information Assurance Program and vetted through an interagency working group that includes members from the Department of Defense, Department of Commerce, Department of Justice, and the National Infrastructure Protection Center. The initiative requires only final coordination of the information flow processes from the DOD CERT to state Army National Guard organizations.

Information is available at the national level that is useful in protecting critical cyber infrastructures. This same information is needed at the state and local levels. Unfortunately, a universally accepted mechanism does not exist to collect, manage, and distribute this needed information across all sectors within states and regions. The

National Guard is constitutionally established to support both federal and state missions and was therefore the logical conduit for information flow between the national and state levels. This initiative would expand that role to encompass protection from cyber threats. As a state agency, the National Guard is responsible to the state governor for providing assistance in state and local crisis and emergency operations. As an immediate response in support of state and local populations, the National Guard is the logical partner for planning and executing emergency operations to ensure readiness and the safety of citizens.

DOD is prepared to share cyber protection information with those organizations that are involved in the operation of the critical infrastructures upon which DOD, including the state National Guards, depends to accomplish its missions. Under the ISIP concept of operations, information generated from the DOD CERT will be pushed downward through state National Guard organizations to state EOC or CERT for appropriate dissemination. Potentially, state and local public and private sector entities could act as sensors providing early warning information upward, thereby enhancing DOD situational awareness.

Appendix A -- Army National Guard, Computer Emergency Response Teams

ARNG INFORMATION OPERATIONS ELEMENTS BY STATE				
STATES	ELEMENT	AUTHORIZED PERSONNEL	TOTALS	REMARKS
AL	State Cert	7	7	STARC, para 12K
AK	State Cert	7	7	STARC, para 12K
AR	Bde IO Section	4	11	
	State Cert	7		STARC, para 12K
AZ	State Cert	7	7	STARC, para 12K
CA	Div IO Section	6	13	
	State Cert	7		STARC, para 12K
CO	State Cert	7	7	STARC, para 12K
CT	State Cert	7	7	STARC, para 12K
DE	State Cert	7	7	STARC, para 12K
DC	State Cert	7	7	STARC, para 12K
FL	Bde IO Section	4	11	
	State Cert	7		STARC, para 12K
GA	Bde IO Section	4	11	
	State Cert	7		STARC, para 12K
GU	State Cert	7	7	STARC, para 12K
HI	Bde IO Section	4	11	
	State Cert	7		STARC, para 12K
IA	Field Support Team	10	17	
	State Cert	7		STARC, para 12K
ID	Bde IO Section	4	11	
	State Cert	7		STARC, para 12K
IL	State Cert	7	7	STARC, para 12K
IN	Div IO Section	6	17	
	Bde IO Section	4		
	State Cert	7		STARC, para 12K
KY	State Cert	7	7	STARC, para 12K
KS	Div IO Section	6	13	
	State Cert	7		STARC, para 12K
LA	Bde IO Section	4	11	
	State Cert	7		STARC, para 12K
MA	Field Support Team	10	17	
	State Cert	7		STARC, para 12K
MD	Field Support Team	10	17	
	State Cert	7		STARC, para 12K
ME	State Cert	7	7	STARC, para 12K
MI	State Cert	7	7	STARC, para 12K
MN	Div IO Section	6	13	
	State Cert	7		STARC, para 12K
MO	Field Support Team	10	17	DA to issue the UIC
	State Cert	7		STARC, para 12K
MS	Bde IO Section	4	11	

	State Cert	7		STARC, para 12K
MT	State Cert	7	7	STARC, para 12K
NC	Bde IO Section	4	11	
	State Cert	7		STARC, para 12K
ND	State Cert	7	7	STARC, para 12K
NE	State Cert	7	7	STARC, para 12K
NH	State Cert	7	7	STARC, para 12K
NJ	State Cert	7	7	STARC, para 12K
NM	State Cert	7	7	STARC, para 12K
NV	State Cert	7	7	STARC, para 12K
NY	Div IO Section	6	17	
	Bde IO Section	4		
	State Cert	7		
OH	State Cert	7	7	STARC, para 12K
OK	Bde IO Section	4	11	
	State Cert	7		
OR	Bde IO Section	4	11	
	State Cert	7		STARC, para 12K
PA	Div IO Section	6	13	
	State Cert	7		STARC, para 12K
PR	State Cert	7	7	STARC, para 12K
RI	State Cert	7	7	STARC, para 12K
SC	Bde IO Section	4	11	
	State Cert	7		STARC, para 12K
SD	State Cert	7	7	STARC, para 12K
TN	Bde IO Section	4	11	
	State Cert	7		STARC, para 12K
TX	Field Support Team	10	23	
	Div IO Section	6		
	State Cert	7		
UT	State Cert	7	7	STARC, para 12K
VA	Div IO Section	6	66	
	Center of Excellence	8		
	Ops and Plans Section	4		Para 005A
	VAT	10		Para 005B
	VAT	10		Para 005C
	LIWA Cert	7		Para 005E
	LIWA Cert	7		Para 005F
	State Cert	7		STARC, para 12K
	NGB-CERT	7		Para 005D
VI	State Cert	7	7	STARC, para 12K
VT	Center of Excellence	8	52	
	IO Training Battalion	27		
	VAT	10		
	State Cert	7		STARC, para 12K
WA	Field Support Team	10	59	
	Field Support Team	10		
	VAT	10		
	VAT	10		

	Center of Excellence	8		
	Bde IO Section	4		
	State Cert	7		STARC, para 12K
WI	State Cert		7	STARC, para 12K
WV	State Cert		7	STARC, para 12K
WY	State Cert		7	STARC, para 12K
	JWRAC	8	8	
TOTALS				690

Identification of ARNG IO Elements	# Soldiers	# Elements	Totals
Bde Information Operations Section	4	15	60
Div Information Operations Section	6	8	48
Centers of Excellence (COE)	8	3	24
Field Support Team (FST)	10	7	70
Joint Web Risk Assessment Cell (JWRAC)	8	1	8
NGB Computer Emergency Response Team (CERT)	7	1	7
LIWA Computer Emergency Response Team (CERT)	7	2	14
STATE Computer Emergency Response Team (CERT)	7	54	378
Operations and Plans Section	4	1	4
Training Battalion	27	1	27
Vulnerability Assessment Team (VAT)	10	5	50
TOTALS			690